2. Теория Галуа

Расширения полей.

$K/k \overset{\text{def}}{\Leftrightarrow}$ фиксировано вложение $k \hookrightarrow K$.

Гомоморфизм $\sigma : K/k \to L/k$ расширений одного и того же основного поля $\overset{\text{def}}{\Leftrightarrow}$ вложение $K \hookrightarrow L$, коммутирующее с вложениями основного поля в K и в L.

Если $P(T) \in k[T]$, $\alpha \in K$, и $P(\alpha) = 0$, то $P(\sigma(\alpha)) = 0$

Алгебраический элемент в $K/k \overset{\text{def}}{\Leftrightarrow}$ $\alpha \in K$ такой,что $\exists P \in k[T] \ |P(\alpha) = 0$.

Алгебраическое расширение $K/k \overset{\text{def}}{\Leftrightarrow}$ все элементы K алгебраичны над k.

Конечное расширение $\overset{\text{def}}{\Leftrightarrow}$ $\dim_k K$ конечна. Она называется степенью расширения $[K : k]$. Если K/k и L/K конечны, то L/k тоже конечно, и $[L : K][K : k] = [L : k]$. Конечное расширение алгебраично.

Расширения, порожденные одним алгебраическим элементом.

k_P - конструкция. $P \in k[T]$ неприводим степени ≥ 1. Тогда $k_P \overset{\text{def}}{=} k[T]/(P)$ - поле (так как (P) максимален). $[k_P : k] = \deg P$.

$k(\alpha)$ - конструкция. K/k -расширение, $\alpha \in K$. $k(\alpha) \overset{\text{def}}{=}$ { минимальное подполе K, содержащее k и α}.

Если α алгебраичен над k, то однозначно определен унитарный неприводимый полином $P_{\alpha, K/k} \in k[T]$ со свойством $P_\alpha(\alpha) = 0$. При этом $k_{P_\alpha} \simeq k(\alpha) \simeq k[\alpha]$ (где $k[\alpha]$ - минимальное подкольцо K,содержащее k и α}.

Свойства алгебраических расширений.

Пусть K/k -расширение. Для любого семейства $\{\alpha_{i,\, i \in I}\}$ элементов K (не обязательно алгебраических над k) можно так же,как выше, определить порожденное ими подполе $k(\{\alpha_i\}) \subset K$ и соответствующее подрасширение. Любой элемент $\alpha \in k(\{\alpha_i\})$ представим (неоднозначно) в виде $\alpha = \frac{P(\{\alpha_i\})}{Q(\{\alpha_i\})}$, где P и Q -полиномы от $\{T_i,\ i \in I\}$ и $Q(\{\alpha_i\}) \neq 0$.

Если K/k порождено конечным числом алгебраических элементов, то оно конечно.

Если K/k порождено любым числом алгебраических элементов, то оно алгебраично.

Если L/K и K/k алгебраичны, то L/k алгебраично.

Алгебраическое замыкание.

Поле K алгебраически замкнуто $\overset{\text{def}}{\Leftrightarrow}$ но не имеет алгебраических расширений $\Leftrightarrow$ $K[T]$ не содержит неприводимых полиномов степени выше 1.

Теорема (2.12). $\forall k\, \exists\, \overline{k}/k$ такое,что $\overline{k}$ алгебраично над k и алгебраически замкнуто.

Гомоморфизмы расширений.

Определение. $\Sigma_{K/k}^{L/k} \overset{\text{def}}{=} \mathrm{Hom}(K/k, L/k) \overset{\text{def}}{=}$ множество всех гомоморфизмов $\sigma : K/k \to L/k$.

Если $K = K_P$, то $\Sigma_{K/k}^{L/k} = \{$множество различных корней $P(T)$ в $L\}$.

Теорема (2.16). Пусть K/k алгебраично, а L алгебраически замкнуто. Тогда $\Sigma_{K/k}^{L/k}$ непусто. Если же K/k и L/k оба алгебраичны, а K и L оба алгебраически замкнуты, то любой гомоморфизм $\sigma \in \Sigma_{K/k}^{L/k}$ - изоморфизм.

Основная лемма (2.15): Пусть $k \subset M \subset K$, $K = M(\alpha)$, α алгебраичен над M, L/k алгебраически замкнуто. Тогда любой элемент $\sigma \in \Sigma_{M/k}^{L/k}$ можно продолжить до элемента $\Sigma_{K/k}^{L/k}$.

Сепарабельные расширения.

Пусть K/k алгебраично. $[K : k]_s \overset{\text{def}}{=} \#(\Sigma_{K/k}^{\overline{k}/k})$ - сепарабельная степень K/k. Она может быть конечной или бесконечной

Теорема (2.18).
1) $[L : K]_s[K : k]_s = [L : k]_s$ если все три степени конечны.
2) Еслиf K/k - конечное расширение, то $[K : k]_s \leq [K : k]$.

Конечное расширение K/k называется сепарабельным, если $[K:k]_s = [K:k]$.

Пусть K/k - любое расширение. Алгебраический элемент $\alpha \in K$ сепарабелен над $k \overset{\text{def}}{\Leftrightarrow} k(\alpha)/k$ сепарабельно. Эквивалентно, $P_\alpha(T)$ не имеет кратных корней в $\overline{k}$.

Алгебраическое расширение K/k сепарабельно $\overset{\text{def}}{\Leftrightarrow}$ все его элементы сепарабельны над k. Для конечных расширений это определение эквивалентно предыдущему.

Если $\mathrm{char}(k) = 0$, то любое алгебраическое расширение K/k сепарабельно.

Если $\mathrm{char}(k) = p$ и K/k конечно, то $[K:k] = p^\nu [K:k]_s$ для какого-то неотрицательного целого ν.

Теорема о примитивном элементе.

Пусть K/k - конечное сепарабельное расширение. Тогда $\exists \alpha \in K$ такой, что $K = k(\alpha)$.

Нормальные расширения и расширения Галуа.

Поле разложения $k_{P,\,\mathrm{split}}$ полинома $P \in k[T]$ степени $d \geq 1$ (не обязательно неприводимого) - это расширение K/k такое, что P разлагается в на линейные множители, и при этом K/k порождено его корнями. Поле разложения определено однозначно с точностью до изоморфизма.

Пример: пусть $\deg P = 2$. Если P неприводим, то $k_{P,\,\mathrm{split}} \overset{\sim}{=} k_P$, в противном случае $k_{P,\,\mathrm{split}} = k$.

Алгебраическое расширение K/k называется нормальным, если, эквивалентно
1) Все $\sigma \in \Sigma_{K/k}^{\overline{k}/k}$ имеют один и тот же образ, или
2) Любой неприводимый полином $P \in k[T]$, имеющий корень в K, распадается над K на линейные множители.

Поле разложения полинома - нормальное расширение.

Для нормального расширения K/k элементы множества $\sigma \in \Sigma_{K/k}^{\overline{k}/k}$ могут быть отождествлены с элементами группы автоморфизмов K/k.

Пусть $k \subset K \subset L$ -башня алгебраических расширений. Если L/k нормально, то и L/K нормально. Однако может случиться так, что L/k нормально, а K/k нет, или что K/k и L/K оба нормальны, а L/k нет.

Алгебраическое расширение K/k называется расширением Галуа, если оно нормально и сепарабельно. Его группа автоморфизмов называется группой Галуа $\mathrm{Gal}\,(K/k)$.

Если K/k - конечное расширение Галуа, то $\#\mathrm{Gal}\,(K/k) = [K : k]$.

Основная теорема теории Галуа.

Пусть $H \subset \mathrm{Gal}\,(K/k)$ - подгруппа. Поле неподвижных элементов для неё $K^H \stackrel{\mathrm{def}}{=} \{x \in K \text{ , такие,что } \forall h \in H \;\; h(x) = x\}$.

Теорема (2.31). Пусть K/k - конечное расширение Галуа, $G = \mathrm{Gal}\,(K/k)$ - его группа Галуа. Тогда
1) Имеется взаимнооднозначное соответствие $\{\text{подгруппы } H \subset G\} \leftrightarrow \{$ подполя $k \subset M \subset K\}$, определенное при помощи отображений $H \mapsto K^H$, $\mathrm{Gal}\,(K/M) \leftarrow\shortmid M$.
2) M/k нормально $\Leftrightarrow$ $H \lhd G$ (т.е.. H - нормальная подгруппа).

Примеры.

1) Пусть $P \in k[T]$ - сепарабельный (не обязательно неприводимый) полином степени ≥ 1.

Пусть $K = k_{P,\,\mathrm{split}}$, $P(T) = \prod\limits_{i-1}^{n}(T - \alpha_i)$, $\alpha_i \in K$. Эти данные определяют вложение $\mathrm{Gal}\,(K/k) \hookrightarrow \mathbf{S}_n$, где группа $\mathbf{S}_n$ - группа перестановок корней α_i.

Дискриминантом (унитарного) полинома $P(T) = \prod\limits_{i-1}^{n}(T - \alpha_i)$, $\alpha_i \in \overline{k}$ называется $\Delta_P \stackrel{\mathrm{def}}{=} \prod\limits_{i<j}(\alpha_i - \alpha_j)^2 \in k$. Дискриминант сепарабельного полинома отличен от 0.

Квадратный корень $\delta_P \stackrel{\mathrm{def}}{=} \sqrt{\Delta_P}$ из дискриминанта лежит в $k_{P,\,\mathrm{split}}$ и определен с точностью до знака.
$\delta_P \in k \Leftrightarrow \{$образ $\mathrm{Gal}\,(k_{P,\,\mathrm{split}}/k)$ лежит в подгруппе четных перестановок $\mathbf{A}_n \subset \mathbf{S}_n\}$.

2) Пусть $P \in k[T]$ сепарабелен степени 2. Он неприводим тогда и только тогда, когда $\delta_P \notin k$. В этом случае $k_{P,\,\mathrm{split}} \simeq k_P$ и $\mathrm{Gal}\,(k_{P,\,\mathrm{split}}/k) = \mathbf{Z}/(2)$.

3) Пусть $P \in k[T]$ неприводим и сепарабелен степени 3. Тогда $\delta_P \in k \Leftrightarrow \mathrm{Gal}\,(k_{P,\,\mathrm{split}}/k) = \mathbf{A}_3 \Leftrightarrow\ k_{P,\,\mathrm{split}} \simeq k_P$. Если же $\delta_P \notin k$, то $\mathrm{Gal}\,(k_{P,\,\mathrm{split}}/k) = \mathbf{S}_3$.

4) Пусть k_0 - поле, $K = k_0(t_1, t_2, \ldots, t_n)$ порождено над k_0 n независимыми переменными. Пусть $k = k_0(s_1, s_2, \ldots, s_n)$, где s_i - элементарные симметрические функции от t_i. Тогда K/k - поле разложения полинома $P(T) = \prod_{i=1}^{n}(T - t_i) = \sum_{j=0}^{n-1}(-1)^{n-j}s_{n-j}T^j + T^n$, и $\mathrm{Gal}\,(K/k) \simeq \mathbf{S}_n$.

5) Конечные поля.

Любое конечное поле содержит q элементов, где $q = p^f$, p - простое число, равное характеристике поля, и f натурально.Такое поле определено с точностью до изоморфизма, обозначается $\mathbf{F}_q$, и множество его элементов может быть отождествлено с $\{x \in \Omega | x^q = x\}$, где Ω - алгебраически замкнутое поле характеристики p . $\mathbf{F}_p$ изоморфно кольцу $\mathbf{Z}/(p)$.

Мультипликативная группа $\mathbf{F}_q^*$ циклична порядка $q - 1$.

Если $K/\mathbf{F}_q$ - расширение степени m, то это расширение Галуа, и $\mathrm{Gal}\,(K/\mathbf{F}_q) \simeq \mathbf{Z}/(m)$. Она порождена относительны гомоморфизмом Фробениуса Fr_q, возводящим элементы $\overline{\mathbf{F}_q}$ в q-ю степень.

6) Основная теорема алгебры (2.35).
$\overline{\mathbf{R}} = \mathbf{R}_{T^2+1}$.

7) Круговые расширения.

Пусть n - натуральное число, k - поле характеристики 0 или такой,что она не делит n. Поле разложения полинома $P(T) = T^n - 1$ называется круговым расширением k. Корни полинома P в $\overline{k}$ называются корнями из 1 степени n. Они образуют циклическую группу порядка n, любая её образующая ζ называется примитивным корнем. Если n просто, то все корни, кроме 1, примитивны.

$k_{P,\,\mathrm{split}}$ - расширение Галуа, $k_{P,\,\mathrm{split}} = k(\zeta)$ и определено вложение $l : \mathrm{Gal}\,(k(\zeta)/k) \hookrightarrow (\mathbf{Z}/(n))^*$ (по формуле $\sigma(\zeta) = \zeta^{l(\sigma)}$).

Полином $f_d(T) = \prod\limits_{(\text{order of}\,\omega)=d} (T - \omega)$ называется круговым полиномом порядка d. Коэффициенты f_d лежат в образе естественного гомоморфизма $\mathbf{Z} \to k$.
$deg f_d = \phi(d)$. $T^n - 1 = \prod\limits_{d|n} f_d(T)$.
Теорема (2.40). f_d неприводим над $\mathbf{Q}$.

Любое квадратичное расширение $\mathbf{Q}$ есть подполе кругового расширения. Это следует из того, что квадрат гауссовой суммы $\tau_p \overset{\text{def}}{=} \sum\limits_{a \mod p} \left(\frac{a}{p}\right) \zeta^a$ равен $(-1)^{\frac{p-1}{2}} p$.

На самом деле любое расширение Галуа поля $\mathbf{Q}$, группа Галуа которого коммутативна, вкладывается в некоторое круговое расширение (теорема Кронекера - Вебера).

Характеристический полином, норма и след.
Пусть K/k - конечное расширение, $\alpha \in K$. Умножение на α определяет линейное преобразование k-векторного пространства K. Его характеристический полином называется характеристическим полиномом α (обозначение $\chi_{\alpha,\,K/k}(T)$), детерминант - нормой α $(N_{K/k}(\alpha))$, а след - следом α $(Tr_{K/k}(\alpha))$.

$N : K^* \to k^*$ и $Tr : K^+ \to k^+$ - гомоморфизмы групп.

Если $\chi_{\alpha,\,K/k}(T) = \sum\limits_{i=0}^{n-1} a_i T^i + T^n$, то $Tr_{K/k}(\alpha)) = -a_{n-1}$ и $N_{K/k}(\alpha) = (-1)^n a_0$

Если $[K : k] = n$ и $\alpha \in k$, то $\chi_{\alpha,\,K/k}(T) = (T - \alpha)^n$, $N_{K/k}(\alpha) = \alpha^n$, $Tr_{K/k}(\alpha) = n\alpha$.

Если $[K : k] = n$, $\alpha \in K$, а степень α над k равна d (то есть $\deg P_{\alpha,\,K/k} = d$), то $\chi_{\alpha,\,K/k} = P_{\alpha,\,K/k}^{\frac{n}{d}}$.

Если K/k сепарабельно, то норму и след можно сосчитать по формулам: $N_{K/k}(\alpha) = \prod\limits_{\sigma \in \Sigma_{K/k}^{\bar{k}/k}} \sigma(\alpha)$, $Tr_{K/k}(\alpha) = \sum\limits_{\sigma \in \Sigma_{K/k}^{\bar{k}/k}} \sigma(\alpha)$

Циклические расширения.

Циклическим расширением называется конечное расширение Галуа с циклической группой Галуа.

Линейная независимость характеров (2.44). Пусть C - произвольная группа, K - любое поле. Пусть $\chi_1, \ldots, \chi_n : C \to K^*$ -различные гомоморфизмы. Тогда отображения χ_i линейно независимы над K.

Теорема Гильберта 90. Пусть K/k - циклическое расширение, σ - образующая $\mathrm{Gal}\,(K/k)$, $\alpha \in K$. Тогда $N_{K/k}(\alpha) = 1 \Leftrightarrow \exists \beta \in K$ such that $\alpha = \frac{\sigma(\beta)}{\beta}$.

Теорема (2.46). Пусть $\mathrm{char}k = 0$ или $(\gcd(\mathrm{char}(k), n) = 1$. Предположим, что $\zeta \in \overline{k}$ - примитивный корень из 1 степени n - содержится в k. Тогда
1) K/k циклично степени $n \Rightarrow \exists b \in k$, такое,что $K \simeq k_{T^n - b}$.
2) $\forall b \in k$ $k_{T^n - b,\,\mathrm{split}}$ - циклично некоторой степени d, $d|n$.

Теорема Гильберта 90, аддитивная версия (лемма к 2.47). Пусть K/k циклично степени n , σ - образующая $\mathrm{Gal}\,(K/k)$, $\alpha \in K$. Тогда $Tr_{K/k}(\alpha) = 0 \Leftrightarrow \exists \beta \in K$ такой, что $\alpha = \sigma(\beta) - \beta$.

Теорема (2.47). Пусть $\mathrm{char}(k)$=p. Тогда
1) K/k циклично степени $p \Rightarrow \exists b \in k$, такое, что $K \simeq k_{T^p - T - b}$.
2) $\forall b \in k$ $T^p - T - b$ либо неприводим, либо полностью распадается в $k[T]$. В первом из случаев $k_{T^p - T - b}$ циклично степени p.

Для описания циклических расширений степени p^k над полем характеристики p при $k > 1$ нужны векторы Витта.

Ограничение группы Галуа.

Теорема (2.48). Пусть K/k - конечное расширение Галуа, M/k - любое расширение (не обязательно алгебраическое). Предположим, что K and M оба содержатся в некотором большем поле $\widetilde{k}$. Пусть $KM \subset \widetilde{k}$ - композит полей K и M (т.е. наименьшее подполе $\widetilde{k}$, содержащее и K, и M).
Тогда KM/M - конечное расширение Галуа, и $\mathrm{Gal}\,(KM/M) = \mathrm{Gal}\,(K/K \bigcap M)$.

Решение уравнений в радикалах.

Пусть $K/\mathbf{Q}$ - конечное расширение, $L/\mathbf{Q}$ - наименьшее расширение Галуа, содержащее K. Расширение $K/\mathbf{Q}$ назывется разрешимым, если $\mathrm{Gal}\,(L/\mathbf{Q})$ - разрешимая группа (т.е. существует композиционный ряд $\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_r = G = \mathrm{Gal}\,(L/\mathbf{Q})$ такой, что $\forall i,\ 1 \leq i \leq r,\ G_i/G_{i-1}$ - циклическая группа).

С другой стороны, пусть $P(T) \in \mathbf{Q}[T]$ - неприводимый полином. Уравнение $P(X) = 0$ разрешимо в радикалах, если существует поле $L \supset \mathbf{Q}_{P,\,\mathrm{split}}$ и последовательность подполей $\mathbf{Q} = L_0 \subset L_1 \subset \cdots \subset L_s = L$ такая, что $\forall i,\ 1 \leq i \leq s,\ L_i = L_{i-1}(\alpha)$, где α - корень полинома $T^m - a = 0$ при некоторых $a \in L_{i-1}$ и $m \in \mathbf{Z}_{>1}$.

Теорема (2.51). Уравнение $P(X) = 0$ разрешимо в радикалах $\Leftrightarrow \mathbf{Q}_P/\mathbf{Q}$ - разрешимое расширение.

Разложение тензорного произведения.

Теорема (2.52). Пусть K/k - конечное сепарабельное расширение, M/k - любое расширение. Тогда существует изоморфизм M - алгебр $K \otimes_k M \simeq \oplus M_i$, где M_i - конечные расширения M вида $M_{P_i},\ \ P_i \in M[T],\ \ \sum \deg P_i = [K : k]$. Набор $\{M_i\}$ определён однозначно с точностью до перестановки и (неканонических) изоморфизмов.

Форма следа.

Теорема (2.53.) Пусть K/k - конечное расширение. Если оно несепарабельно, то $Tr : K \to k$ - нулевое отображение, а если сепарабельно, то $Tr(ab) : K \times K \to k$ - невырожденная симметричная билинейная форма.